APPOSITE TECHNOLOGIES

NETROPY CYBERATTACK

Security teams from all industries, enterprise and Government, need to know with certainty that their cyber defenses are up to the challenge of today's evolving threat landscape. So how can you verify your security in a fast, effective, and affordable way?

Netropy CyberAttack is a complete security test solution designed to evaluate the performance of network security architecture, validate DDoS defenses, and optimize security devices like Next-Gen firewalls and WAFs. Simulate real-world traffic and malicious attacks at massive scale to identify vulnerabilities and measure the ability of security devices and policies to protect against threats.

Optimize Network Performance and Harden Defenses with One Complete Solution

Comprehensive Security Testing

By combining advanced security testing, performance benchmarking, and traffic generation capabilities, Netropy CyberAttack empowers organizations to validate security defenses, ensure reliable attack detection, and evaluate response effectiveness—all in a controlled lab environment.

Emulate Real-World Threats. Generate attack traffic and legitimate application traffic simultaneously to test under the most realistic conditions and worst-case scenarios. Simulate large-scale DDoS attacks, malware, CVEs and more.

Conduct Layer 2-7 Testing. Simulate multi-vector, multi-stage attacks against layers 2-7. Generate L2-3 attacks to test network-level vulnerabilities to prevent network disruption and unauthorized access. Launch L4-7 campaigns targeting protocols and applications to protect data, user sessions, and app functionality.

Test and Measure Defenses Against Distributed Denial of Services (DDoS) Attacks. Simulate DDoS attacks to evaluate the effectiveness of prevention and mitigation strategies. See how well DDoS protection, Web Application Firewalls (WAFs) and other tools detect, block, and minimize the impact of attacks.

Configure Global Threats. Generate large volumes of legitimate and malicious traffic originating from specific geographic regions to test location-based security policies and identify potential entry points for attackers.

Access an Up-to-date and Ever-evolving Library of Cybersecurity Threats. The dynamic Attack Library includes pre-defined attack patterns, including zero-day, DDoS, malware, CVEs and more based on current cyber intelligence.

Benchmarking Performance Under Stress

Push network and security devices to their limits to validate performance under real-world conditions. Generate authentic application traffic and recreate complex network scenarios to identify potential bottlenecks and weak points before deployment.

Measure Classic Network Metrics. Measure throughput, packet loss, latency, and jitter while applying various application and attack scenarios. Emulate millions of endpoints and generate authentic traffic to uncover performance issues and improve system resilience.

Capture, Reproduce, and Amplify Production Traffic. Capture production network conditions and convert them into dynamic traffic streams to help find and eliminate performance bottlenecks. Transform single traffic captures into millions of flows to assess device and system capacity under real-world loads.

Optimize the Performance and Functionality of Application-aware Devices and Systems. Validate the performance of application-aware devices like firewalls and SD-WAN gateways at scale using an extensive library of pre-defined application flows.

Ensuring Quality of Service (QoS)

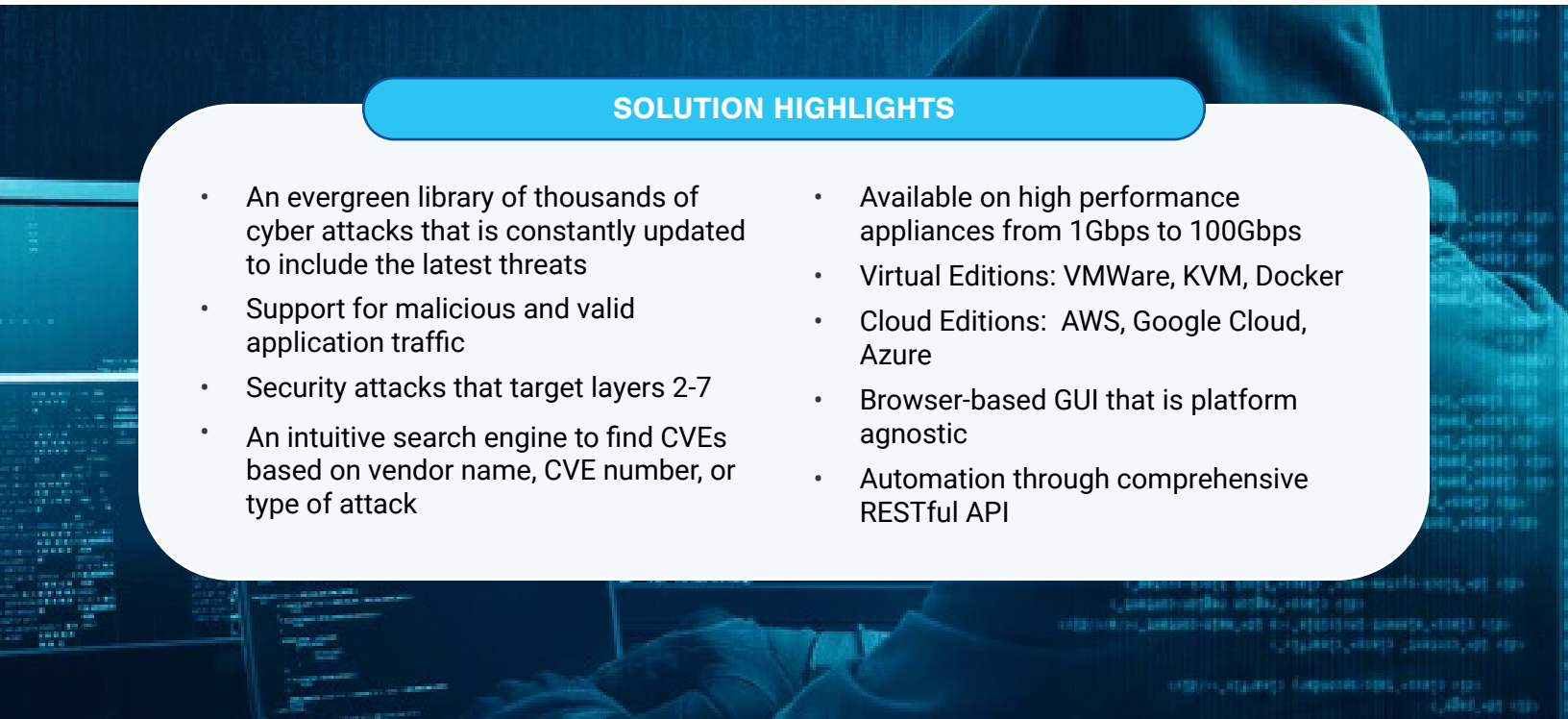
Simulate production-level application traffic mixes to test the effectiveness of traffic management strategies and measure the impact of QoS configurations on application performance and availability.

Validate QoS Policies. Measure performance metrics on the application level to ensure the network is delivering the required level of performance for different types of applications.

Stress Test the Network. Over saturate the network to ensure that critical applications are given priority when network resources become limited.

Proactively Resolve Problems. Detect and resolve performance and security issues early to prevent costly downtime and service disruptions. Recreate customer issues to quickly solve support incidents and improve service reliability.

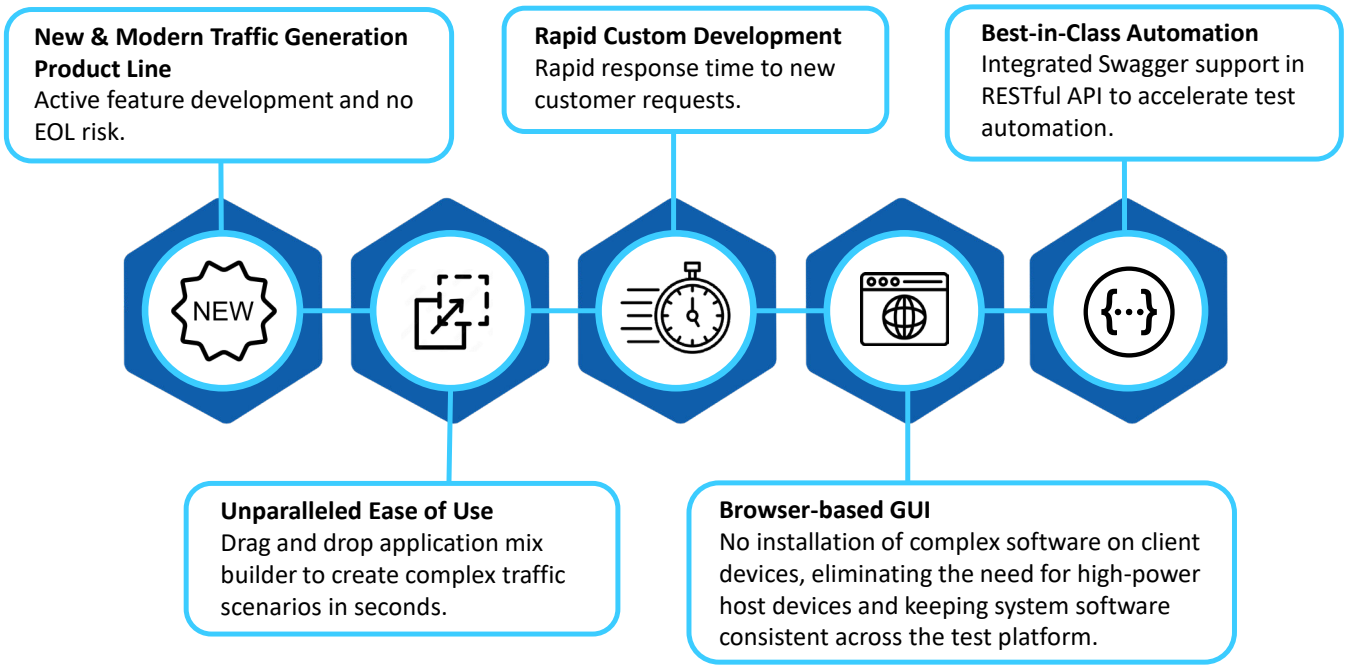
Ensure Critical Application Security. Simulate various traffic scenarios to verify that critical applications maintain security and functionality, even under stress or during simulated attacks.



SOLUTION HIGHLIGHTS

- An evergreen library of thousands of cyber attacks that is constantly updated to include the latest threats
- Support for malicious and valid application traffic
- Security attacks that target layers 2-7
- An intuitive search engine to find CVEs based on vendor name, CVE number, or type of attack
- Available on high performance appliances from 1Gbps to 100Gbps
- Virtual Editions: VMWare, KVM, Docker
- Cloud Editions: AWS, Google Cloud, Azure
- Browser-based GUI that is platform agnostic
- Automation through comprehensive RESTful API

Advantages of Netropy CyberAttack



Available Appliances for Netropy CyberAttack

Model	Speed and Ports
Netropy CyberAttack N61	2x 1Gbps ports RJ45
Netropy CyberAttack 10G2	4x 10Gbps ports SFP+
Netropy CyberAttack 10G4	8x 10Gbps ports SFP+
Netropy CyberAttack 100G	2x 100Gbps ports QSFP28
Netropy CyberAttack 100G2	4x 100Gbps ports QSFP28
Netropy CyberAttack VE	Virtual Edition
Netropy CyberAttack CE	Cloud Edition

ABOUT APPOSITE

Apposite has been in business for over 20 years and has helped customers around the globe from telecoms to system integrators, technology vendors and large enterprises. Our modern, easy-to-use test solutions enable teams to set up performance tests quickly and easily and trust the results.

Apposite Technologies

4223 Glencoe Ave B121, Marina Del Rey, CA 90292 USA